

Prolongations of quasigroups

V.A. Shcherbacov

July 22, 2015

Abstract

We give an overview of various prolongations of quasigroups. Two step prolongation procedure is proposed.

2000 Mathematics Subject Classification: 20N05, 05B15

Key words and phrases: quasigroup, quasigroup prolongation

In memoriam: Galina Borisovna Belyavskaya
(1940 - 2015).

Given information was prepared for submission at the conference LOOPS'15 (28 June - 04 July, 2015, Ohrid, Macedonia).

1 Quasigroup prolongations

Quasigroup prolongation is quit natural way of construction of a finite quasigroup of order $n+k$ ($k \leq n$) from a quasigroup of order n . We start from some definitions. Mainly we follow [8, 2, 1, 10].

R.H. Bruck proposed to use transversals (n -transversals) for prolongation of a quasigroup [6]. We give Belousov construction of quasigroup prolongation. If transversal elements are situated on main diagonal, we obtain Bruck construction.

Construction 1. *We prolong the Latin square and quasigroup $(Q, *)$ of order 3 to Latin square and corresponding quasigroup (Q', \star) of order 4 in the following way.*

We add additional column from the right and additional row below, transpose in these new cell all marked (transversal) elements in their fixed order and fill all

remaining empty cells by the symbol "4".

1	2	3	
2	3	1	
3	1	2	

 \rightarrow

1	2		3
	3	1	2
3		2	1
2	1	3	

 \rightarrow

1	2	4	3
4	3	1	2
3	4	2	1
2	1	3	4

It is easy to see that the initial Latin square from Construction 1 has more than one transversal. Using colored boxes we "isolated" in the initial Latin square three disjoint transversals.

Example 1.

1	2	3
2	3	1
3	1	2

There exists a possibility to generalize Construction 1 and to make a quasigroup prolongation using $2, 3, \dots, n$ **disjoint** transversals [7, 12]. We demonstrate generalization of Construction 1 on the following examples.

Example 2. We prolong the Latin square of order 3 to Latin square of order 5 in the following way.

Step 1. We add two additional columns from the right and two additional rows below, transpose in these new cell all marked (transversal) elements in their fixed order (i.e, we project these elements along rows and along columns). Notice we can add these two columns and two rows in any suitable place of a given Latin square.

		3	1	2
2			3	1
	1		2	3
1	3	2		
3	2	1		

Step 2.

Fill all empty after transposition transversal cells by the symbols "4, 5". In transversal cells of a fixed transversal we put the same element. Here yellow transversal we fill by the element "4".

4	5	3	1	2
2	4	5	3	1
5	1	4	2	3
1	3	2		
3	2	1		

Step 3. In remaining right bottom empty square we put a quasigroup of order 2 defined on the set $\{4, 5\}$.

4	5	3	1	2
2	4	5	3	1
5	1	4	2	3
1	3	2	5	4
3	2	1	4	5

Modification of Step 1. We can change the order of colored rows and/or columns.

4	5	3	1	2
2	4	5	3	1
5	1	4	2	3
3	2	1	5	4
1	3	2	4	5

Remark 1. *It is clear that by prolongation of Latin squares and quasigroups we can situate additional columns and rows not only from the right and in the bottom of initial Latin square, but in any other suitable place.*

Example 3. We prolong the Latin square of order 3 to Latin square of order 6 in the following way.

Step 1.

We add three additional columns from the right and three additional rows below, transpose in these new cell all marked (transversal) elements in their fixed order.

□	□	□	1	2	3
□	□	□	3	1	2
□	□	□	2	3	1
1	3	2	□	□	□
3	2	1	□	□	□
2	1	3	□	□	□

Step 2.

Fill all remaining empty after transposition transversal cells by the symbols "4, 5, 6" in their "old transversal order", i.e. we put the symbol 4 in all empty cells of light-blue transversal.

6	5	4	1	2	3
4	6	5	3	1	2
5	4	6	2	3	1
1	3	2	□	□	□
3	2	1	□	□	□
2	1	3	□	□	□

Step 3.

In remaining right bottom empty square we put any quasigroup of order 3 defined on the set $\{4, 5, 6\}$.

6	5	4	1	2	3
4	6	5	3	1	2
5	4	6	2	3	1
1	3	2	4	5	6
3	2	1	5	6	4
2	1	3	6	4	5

In more formalized manner construction which is described in Examples 2 and 3 is given in [11]. Using this construction on base of T-quasigroups in [11] many MDS-codes are constructed. A pair of orthogonal quasigroups of order ten is also constructed [11, 13].

2 Belyavskaya modification

G.B. Belyavskaya proposed modification of Bruck-Belousov construction [5, 3, 4].

Construction 2. *We add additional column from the right and additional row below, transpose in these new cells all marked (transversal) elements except one (in our example element 2) in their fixed order and fill all remaining empty cells except one (with coordinates $(n+1, n+1)$) by the symbol "4". The cell with coordinates $(n+1, n+1)$ is filled by the not transposed transversal element.*

1	2	3				→	1	2	□	3				→	1	2	4	3
2	3	1					2	3	1	□					2	3	1	4
3	1	2					3	□	2	1					3	4	2	1
							□	1	3	□					4	1	3	2

Construction 3. *Generalized Belyavskaya construction. It is possible to generalize Belyavskaya construction using more than one disjoint transversal.*

Example 4. We prolong the Latin square of order 3 (Example 1) to Latin square of order 5 using Belyavskaya prolongation construction (Construction 2) that simultaneously is applied to two transversals.

We add two additional columns from the right and two additional rows below, transpose in these new cell all marked (transversal) elements in their fixed order for exception of one element in any transversal. We take element 1 in yellow transversal and take element 1 in green transversal. It is not obligatory that in yellow and green transversal we take equal "exceptional" elements.

Step 1.

1	□	3	□	2
2	□	1	3	□
□	1	□	2	3
□	3	2	□	□
3	2	□	□	□

Step 2.

Fill all remaining empty after transposition transversal cells by the symbols "4, 5". In transversal cells of a fixed transversal we put the same element.

In the bottom of main diagonal write elements "4, 5". Unfortunately here direct generalization of Belyavskaya construction is not possible.

1	4	3	5	2
2	5	1	3	4
4	1	5	2	3
5	3	2	4	1
3	2	4	1	5

Modification of Step 1. We can change the order colored rows and/or columns. For example we have changed 4-th and 5-th rows.

1	4	3	5	2
2	5	1	3	4
4	1	5	2	3
3	2	4	1	5
5	3	2	4	1

Example 5. Using generalized Belyavskaya construction we prolong the Latin square of order 3 to Latin square of order 6 in the following way.

Step 1. We add three additional columns from the right and three additional rows below, transpose in these new cells all marked (transversal) elements in their

fixed order for exception of the element 3 from yellow transversal, the element 3 from green transversal and the element 1 from light-blue transversal.

□	□	□	1	2	3
□	3	□	□	1	2
3	1	□	2	□	□
1	□	2	□	□	□
□	2	1	□	□	□
2	□	3	□	□	□

Step 2. Fill all remaining empty after transposition transversal cells by the symbols "4, 5, 6" in their "old transversal order", i.e. we put the symbol 4 in all empty cells of light-blue transversal and so on.

4	5	6	1	2	3
6	3	5	4	1	2
3	1	4	2	5	6
1	4	2	□	□	□
5	2	1	□	□	□
2	6	3	□	□	□

Step 3. Remaining right bottom empty square we should complete in order to obtain a quasigroup. Bottom part of main diagonal we fill by the elements 3, 3, 1, because namely these elements remain in transversals.

In this case cell (5, 4) can be filled only by the element 6. Remaining is clear for any fan of Sudoku.

4	5	6	1	2	3
6	3	5	4	1	2
3	1	4	2	5	6
1	4	2	3	6	5
5	2	1	6	3	4
2	6	3	5	4	1

3 Prolongation using quasicomplete mappings

I.I. Derienko and W.A. Dudek propose prolongation construction of a quasigroup using quasicomplete mappings [10]. This construction is generalization of Belyavskaya construction on quasicomplete mappings.

Definition 1. Let (Q, \cdot) be a finite quasigroup, σ be a mapping of the set Q . We can construct the mapping $\bar{\sigma}$ in the following way:

$$\bar{\sigma}x = x \cdot \sigma x \quad \text{for all } x \in Q. \quad (1)$$

The mapping $\bar{\sigma}$ is called *conjugated mapping* to the mapping σ .

A mapping σ is *quasicomplete*, if σ is a permutation of a set Q and $\bar{\sigma}(Q)$ contains all elements of Q except one. In this case there exists an element $a \in Q$, called special, such that $a = \bar{\sigma}x_1 = \bar{\sigma}x_2$ for some $x_1, x_2 \in Q$, $x_1 \neq x_2$.

Construction 4. We start from a quasigroup and a quasicomplete mapping, act as in Belyavskaya construction but in the cell with coordinates $(n+1, n+1)$ we write the element $Q \setminus \bar{\sigma}Q$ (the special element).

Example 6. We take the following quasigroup

\cdot	1	2	3	4
1	2	1	3	4
2	3	2	4	1
3	4	3	1	2
4	1	4	2	3

and the following mapping

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Then

$$\bar{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 3 \end{pmatrix},$$

σ is quasicomplete mapping and $Q \setminus \bar{\sigma}Q = \{1\}$. Using Derienko-Dudek construction we obtain

$*$	1	2	3	4	5		$*$	1	2	3	4	5
1	□	1	3	4	2		1	5	1	3	4	2
2	3	2	□	1	4		2	3	2	5	1	4
3	4	□	1	2	3	→	3	4	5	1	2	3
4	1	4	2	3	□		4	1	4	2	3	5
5	2	3	4	□	□		5	2	3	4	5	1

There exists a possibility to generalize Derienko-Dudek construction in Yamamoto spirit.

Example 7. It is clear that the following Latin square has four disjoint quasicomplete mappings. We shall use yellow and green quasi-complete mappings for the prolongation of this Latin square.

2	1	3	4
3	2	4	1
4	3	1	2
1	4	2	3

Step 1.

We add two columns and two rows and transpose there elements of the yellow and green quasi-complete mappings.

□	□	3	4	2	1
□	2	□	1	4	3
4	□	1	□	3	2
1	4	2	3	□	□
2	3	4	□	□	□
3	1	□	2	□	□

Step 2.

We fill empty yellow cells in the initial Latin square by the number 5 and green cells by the number 6. We fill bottom part of main diagonal by the elements 1 and 4 respectively.

5	6	3	4	2	1
6	2	5	1	4	3
4	5	1	6	3	2
1	4	2	3	□	□
2	3	4	□	1	□
3	1	□	2	□	4

Step 3.

Finally we complement obtained partial Latin square to complete Latin square. It is easy to see that it is possible do this in a unique way.

5	6	3	4	2	1
6	2	5	1	4	3
4	5	1	6	3	2
1	4	2	3	6	5
2	3	4	5	1	6
3	1	6	2	5	4

4 Two step mixed procedure

Suppose that a quasigroup of order n has two disjoint transversals. On the first step we can prolong this quasigroup to a quasigroup of order $n + 1$ using Bruck-Belousov or Belyavskaya construction. After this procedure our second transversal passes in complete or quasicomplete mapping (i.e. in n - or $(n - 1)$ -transversal) and we can prolong obtained quasigroup using Bruck-Belousov or Belyavskaya construction, either Derienko-Dudek construction (if we have obtained quasicomplete mapping).

Example 8.

1	2	3
2	3	1
3	1	2

On the first step we use blue transversal and Belyavskaya construction (see Construction 2) and obtain the following Latin square.

1	2	4	3
2	3	1	4
3	4	2	1
4	1	3	2

In this case yellow transversal passes in $(n-1)$ -th transversal (quasicomplete mapping)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Then

$$\bar{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 2 \end{pmatrix},$$

σ is quasicomplete mapping and $Q \setminus \bar{\sigma}Q = \{4\}$. Using Derienko-Dudek construction we obtain

5	2	4	3	1
2	5	1	4	3
3	4	5	1	2
4	1	3	2	5
1	3	2	5	4

5 Contractions of quasigroups

Procedure which is inverse to prolongation of quasigroups is called contraction of quasigroup. Procedures of contraction of quasigroups make from a quasigroup of order n a quasigroup of order $(n-1)$ or $(n-2)$. It is clear that any procedure of prolongation has its proper "inverse" procedure of contraction. See [4, 3, 9] for details.

Probably procedures of prolongation and contraction of quasigroups can be used in cryptography.

References

- [1] V.D. Belousov. Extensions of quasigroups. *Bul. Akad. Stiince RSS Moldoven*, (8):3–24, 1967. (in Russian).
- [2] V.D. Belousov. *Foundations of the Theory of Quasigroups and Loops*. Nauka, Moscow, 1967. (in Russian).
- [3] G.B. Belyavskaya. Contraction of quasigroups. I. *Bul. Akad. Stiince RSS Moldoven*, (1):6–12, 1970. (in Russian).
- [4] G.B. Belyavskaya. Contraction of quasigroups. II. *Bul. Akad. Stiince RSS Moldoven*, (3):3–17, 1970. (in Russian).
- [5] G.B. Belyavskaya. Generalized extension of quasigroups. *Mat. Issled.*, 5(2):28–48, 1970. (in Russian).
- [6] R.H. Bruck. Some results in the theory of quasigroups. *Trans. Amer. Math. Soc.*, 55:19–52, 1944.
- [7] M. Damm. *Total anti-symmetrische Quasigruppen*. PhD thesis, Philipps-Universität Marburg, 2004. (in German).
- [8] J. Dénes and A. D. Keedwell. *Latin Squares and their Applications*. Akadémiai Kiadó, Budapest, 1974.
- [9] I. I. Deriyenko and W. A. Dudek. Contractions of quasigroups and Latin squares. *Quasigroups Relat. Systems*, 21(2):165–174, 2013.
- [10] Ivan I. Deriyenko and Wieslaw A. Dudek. On prolongations of quasigroups. *Quasigroups Relat. systems*, 16:187–198, 2008.
- [11] S. Gonsales, E. Couselo, V. T. Markov, and A. A. Nechaev. Recursive MDS-codes and recursively differentiable quasigroups. *Diskret. Mat.*, 10(2):3–29, 1998. (in Russian).
- [12] Koichi Yamamoto. Generation principles of Latin squares. *Bull. Inst. Internat. Statist.*, 38:73–76, 1961.
- [13] Lie Zhu. A short disproof of Euler’s conjecture concerning orthogonal Latin squares. With editorial comment by A. D. Keedwell. *Ars Combin.*, 14:47–55, 1982.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD–2028 Chişinău
Moldova
Email: scerb@math.md